**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ**
**«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ**
**імені Ігоря СІКОРСЬКОГО»**
**Навчально-науковий фізико-технічний інститут**
**Кафедра математичних методів захисту інформації**

# Проектування, розробка і реалізація криптографічних систем

## Лабораторна робота № 2

зі спеціальності: 113 Прикладна математика
на тему: **Дослідження реалізацій протоколів IPSec**

Виконали:
студенти VI курсу, групи ФІ-32мн
Маринін Іван Павло
Панасюк Єгор
Пелешенко Любов

Київ — 2024

# ЗМІСТ

Вступ ..... 3
1 Основне призначення ..... 4
2 Криптографічні механізми протоколів ..... 8
3 Концепція безпечних асоціацій (Security Associations, SA), бази даних SPD і SAD ..... 10
4 Особливості структури заголовків протоколів AH та ESP в тунельному і транспортному режимах ..... 12
5 Домен інтерпретації DOI ..... 17
6 Зареєстровані алгоритми для стеку протоколів IPSec ..... 19
7 Основні схеми застосування протоколів IPSec ..... 21
8 IPSec для побудови VPN-тунелів ..... 23
9 Контрольні запитання ..... 25
Висновки ..... 27

# ВСТУП

**Мета**

Дослідити особливості реалізації криптографічних механізмів протоколів IPSec.

**Постановка задачі**

Провести дослідницьку роботу з метою аналізу особливостей реалізації криптографічних механізмів протоколів IPSec. Описати основне призначення протоколів IPSec, їх місце в мережевій моделі OSI та взаємодію зі стеком протоколів TCP/IP та ін. Дослідити архітектуру стеку протоколів IPSec. Описати призначення, особливості та відмінності криптографічних механізмів протоколів AH, ESP, ISAKMP, IKE, IKEv2, KINK та ін. Проаналізувати концепцію безпечних асоціацій (SA), її особливості та бази даних SPD і SAD (їх призначення та способи заповнення і використання). Дослідити детально особливості структури заголовків протоколів AH і ESP в тунельному та транспортному режимах з повним описанням їх полів та можливих значень. Визначити особливості обробки вхідних та вихідних IPSec-пакетів для кожного з протоколів та режимів. Дослідити нижній рівень архітектури стеку протоколів IPSec – домен інтерпретації DOI. Визначити зареєстровані алгоритми автентифікації, шифрування, геш-функцій та ін. криптографічних алгоритмів для стеку протоколів IPSec. Визначити та описати особливості основних схем застосування протоколів IPSec: хост-хост, шлюз-шлюз та хост-шлюз. А також використання протоколів IPSec для побудови VPN-тунелів.

# 1 ОСНОВНЕ ПРИЗНАЧЕННЯ



IPSec (Internet Protocol Security) — це набір протоколів, що забезпечує захист даних на мережевому рівні шляхом їх шифрування та автентифікації. Основні цілі IPSec:

1) **конфіденційність**: забезпечується за допомогою шифрування даних

2) **цілісність**: гарантується тим, що дані не змінюються під час передачі.

3) **автентифікація**: перевірка джерела даних і їх отримувача.

4) **тунелювання**: IPSec підтримує тунелювання, що дозволяє інкапсулювати IP-пакети в іншому протоколі, наприклад, GRE (Генераційна інкапсуляція маршрутизації) або L2TP (Протокол тунелювання рівня 2).

5) **гнучкість**: IPSec можна налаштувати для забезпечення безпеки для широкого спектра мережевих топологій, включаючи точка-точка, сайт-сайт та підключення віддаленого доступу.

6) **взаємодія**: IPSec є відкритим стандартним протоколом, що означає, що його підтримує широкий спектр постачальників і його можна використовувати в неоднорідних середовищах.

7) **управління ключами**: IPSec надає послуги управління ключами, включаючи обмін ключами та відкликання ключів, щоб забезпечити безпечне управління криптографічними ключами.

IPSec використовується для захисту даних під час їх передачі через Інтернет. IPSec створює захищені з'єднання між пристроями, забезпечуючи збереження інформації, що обмінюється, у безпеці від несанкціонованого доступу. IPSec працює в основному двома способами: у режимі транспорту та у тунельному режимі.

Для забезпечення безпеки IPSec використовує два основних протоколи: AH (Заголовок аутентифікації) та ESP (Інкапсульоване вантажне безпеки). Обидва протоколи є дуже корисними, оскільки Заголовок аутентифікації перевіряє дані, щоб визначити, чи вони надходять з надійного джерела і чи не були змінені, а ESP виконує аутентифікацію та шифрує дані, щоб ускладнити їх читання.

Для шифрування IPSec використовує криптографічні ключі. Вони можуть бути створені та поділені за допомогою процесу, відомого як IKE (Обмін ключами в Інтернеті), що забезпечує наявність у обох пристроїв правильних ключів для встановлення захищеного з'єднання.

Коли два пристрої спілкуються, використовуючи IPSec, вони спочатку ініціюють з'єднання, надсилаючи один одному запит. Після цього вони взаємно вирішують питання захисту даних, використовуючи паролі або цифрові сертифікати. Тепер вони встановлюють безпечний тунель для комунікації. Як тільки тунель налаштований, дані можуть бути безпечно передані, оскільки IPSec шифрує дані та також перевіряє їх цілісність, щоб гарантувати, що дані не були змінені. Після завершення зв'язку пристрої можуть закрити безпечне з'єднання. Таким чином, IPSec працює.

Схематично роботу IPSec зображено на Рисунку 1.1

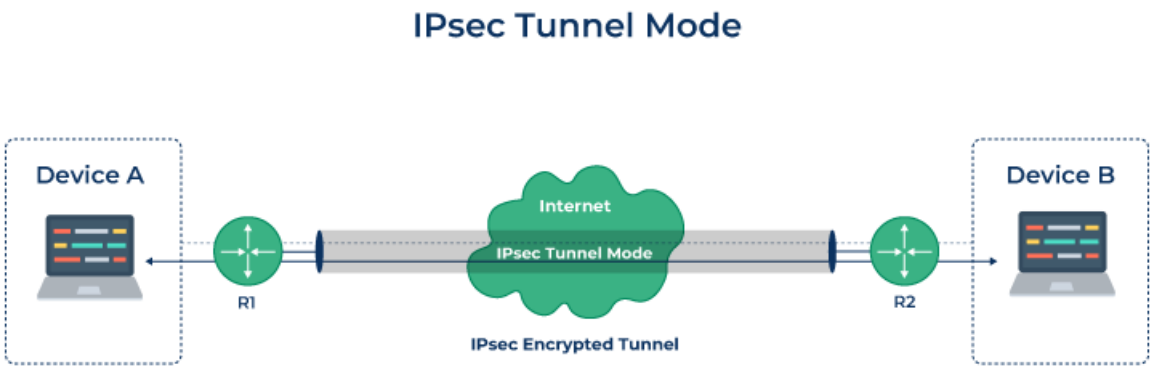
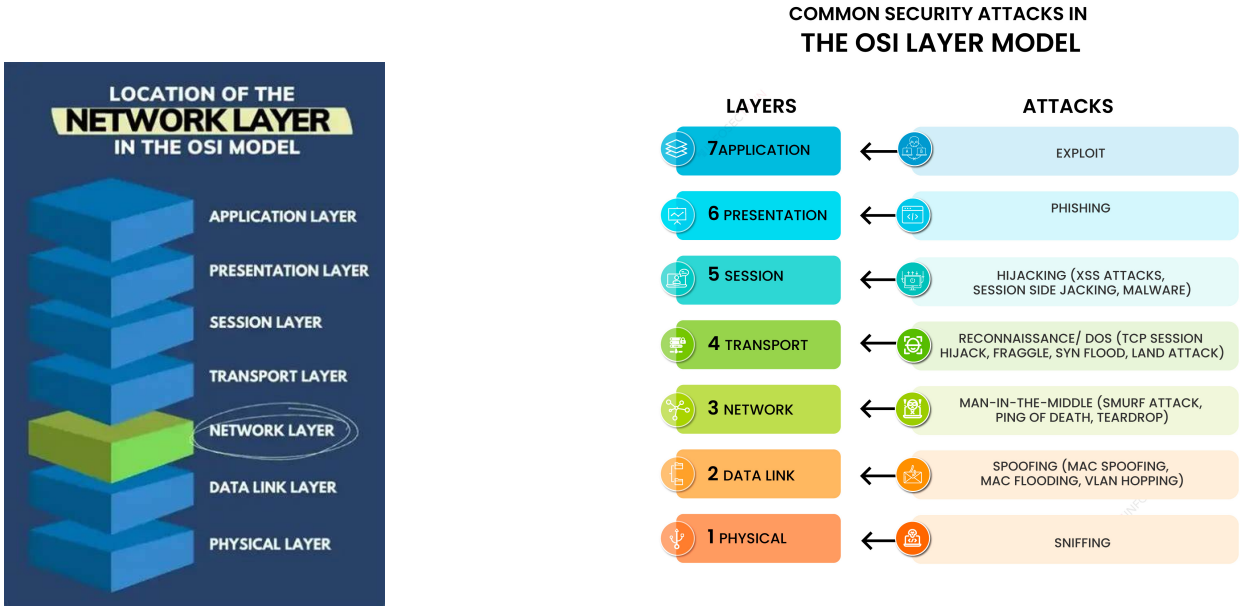



**Рисунок 1.1** – Схема роботи IPSec

IPSec працює на мережевому рівні, тобто на 3-ому, моделі OSI (Рисунок 1.2). Це дозволяє йому забезпечувати захист без залежності від застосункових протоколів або протоколів транспортного рівня. Таким чином, IPSec забезпечує універсальний захист для всіх протоколів, які використовують IP для передавання даних.




(а) (б)

**Рисунок 1.2** – IPSec у моделі OSI.

Якщо ж говорити про взаємодію зі стеком TCP/IP, то у там IPSec інтегрується на рівні IP-протоколу (IPv4 або IPv6). Це дозволяє йому шифрувати і захищати IP-пакети незалежно від протоколів транспортного рівня, таких як TCP або UDP.

**Основні компоненти архітектури IPSec**

Архітектура IPSec складається з чотирьох основних функціональних компонентів:

• **Протоколи забезпечення безпеки (Security Protocols)**: Authentication Header (AH): забезпечує автентифікацію та цілісність IP-пакетів, Encapsulating Security Payload (ESP): забезпечує шифрування, автентифікацію та цілісність даних.

• **Протоколи управління ключами**: Internet Key Exchange (IKE): використовується для аутентифікації сторін, встановлення захищених сесій, та управління ключами.

• **Політики безпеки (Security Policies)**: адаються в Security Policy Database (SPD). Ці політики визначають, як обробляються пакети (шифрування, автентифікація або пропуск без захисту).

• **Бази даних IPSec**: Security Association Database (SAD): містить параметри активних асоціацій безпеки. SPD (Security Policy Database): визначає правила безпеки, які застосовуються до IP-трафіку.

Архітектура IPSec організована у вигляді функціональних рівнів, які забезпечують гнучкість і розширюваність:

(а) **Security Policy Database (SPD)**: визначає, як обробляти вхідні та вихідні пакети.

- *Пропуск без змін (Bypass)*: для довіреного трафіку.
- *Заблокувати (Discard)*: для небажаного трафіку.
- *Захистити (Protect)*: для трафіку, який потребує IPSec.

(б) **Security Association (SA)**: є основним елементом IPSec, який описує параметри для обробки пакету. Встановлюється для кожного напряму трафіку (вихідного або вхідного). Кожна SA визначається трьома параметрами:

- *Ідентифікатор безпеки (SPI).*
- *IP-адреса віддаленого вузла.*
- *Тип протоколу (AH або ESP).*

(в) **Internet Key Exchange (IKE)**: є протоколом управління ключами. Його завдання полягає у налаштуванні захищеного каналу для передачі параметрів IPSec та генерації (разом із оновленнями) ключів. Працює у 2 етапи: створення захищеного каналу управління та встановлення SAs для захисту даних.

(г) **Протоколи AH та ESP**:

*Authentication Header (AH)*: додає заголовок автентифікації до IP-пакету, а також забезпечує цілісність і автентифікацію, але не шифрує дані.

*Encapsulating Security Payload (ESP)*: забезпечує шифрування даних, автентифікацію та цілісність і може працювати в транспортному або тунельному режимі.

Як уже було сказано раніше, IPSec може працювати у 2 режимах, а саме: *транспортний* – захищає лише корисне навантаження IP-пакету і використовується для захисту з'єднань кінцевих вузлів; *тунельний* – інкапсулює весь IP-пакет у новий IP-заголовок і використовується для створення VPN (Virtual Private Network).

Щоби обробити дані в IPSec потрібно дотримуватись наступних принципів: вхідні пакети перевіряються на відповідність політиці у SPD; вихідні пакети обробляються відповідно до SAs, визначених у SAD; шифрування та автентифікація здійснюються відповідно до параметрів, заданих протоколами AH або ESP.

IPSec інтегрується у стек TCP/IP на рівні мережевого протоколу (IP). Він працює як прозорий шар між мережевим і транспортним рівнями, забезпечуючи захист без втручання в роботу застосунків.

У цьому розділі розглянуто призначення, особливості та відмінності криптографічних механізмів таких протоколів як: AH, ESP, ISAKMP, IKE, IKEv2, KINK.

1. **Authentication Header (AH)**.
Забезпечує автентифікацію та цілісність IP-пакетів без шифрування їх вмісту. Він дозволяє гарантувати, що дані не були змінені під час передачі та походять від довіреного джерела.
*Особливості*:
– використовує хеш-функції (наприклад, HMAC-SHA-256) для створення автентифікаційного коду.
– не забезпечує конфіденційність (шифрування).
– захищає IP-заголовок, якщо не використовується NAT (Network Address Translation).
– використовує фіксований номер протоколу 51 в заголовках IP.
*Відмінності*:на відміну від ESP, AH не підтримує шифрування і менш популярний через обмежену функціональність і проблеми сумісності з NAT.

2. **Encapsulating Security Payload (ESP)**.
Забезпечує шифрування, автентифікацію та цілісність IP-пакетів. Він використовується для захисту конфіденційності переданих даних.
*Особливості*:
– підтримує як шифрування (наприклад, AES), так і автентифікацію (HMAC).
– може працювати в транспортному та тунельному режимах.
– захищає лише корисне навантаження (payload) IP-пакету, але не його заголовок (у транспортному режимі).
– використовує фіксований номер протоколу 50 в заголовках IP.
*Відмінності*: на відміну від AH, ESP підтримує шифрування, що робить його більш універсальним, а також у тунельному режимі забезпечує повний захист IP-пакетів.

3. **Internet Security Association and Key Management Protocol (ISAKMP)**.
Протокол управління ключами, який визначає структуру і механізми створення, зміни та видалення Security Associations (SAs).
*Особливості*:
– незалежний від конкретних алгоритмів шифрування та автентифікації.
– працює у поєднанні з IKE, який забезпечує криптографічні алгоритми.
– описує структуру повідомлень і взаємодію, але не механізми захисту.
*Відмінності*: не шифрує і не аутентифікує дані самостійно, а лише управляє процесами обміну ключами.

4. **Internet Key Exchange (IKE)**.
Використовується для створення захищених тунелів між вузлами, які реалізують IPSec, та для управління SAs.

*Особливості*:
– об'єднує функції ISAKMP з конкретними криптографічними алгоритмами.
– працює у двох фазах: захищене налаштування каналу управління (Phase 1) та створення SAs для IPSec (Phase 2).
– підтримує різні механізми автентифікації (наприклад, сертифікати, PSK).
*Відмінності*: IKE є криптографічним розширенням ISAKMP і включає в себе функції управління ключами.

5. **Internet Key Exchange version 2 (IKEv2)**.
IKEv2 є вдосконаленою версією IKE, яка забезпечує підвищену ефективність та безпеку при створенні SAs.
*Особливості*:
– покращений механізм повторної синхронізації тунелів у разі обриву зв'язку.
– менша кількість раундів обміну (до 4 повідомлень) порівняно з IKE.
– вбудована підтримка NAT-Traversal.
– використовує менше ресурсів мережі, що робить його придатним для мобільних пристроїв.
*Відмінності*: IKEv2 швидший і простіший у налаштуванні, ніж IKE, і забезпечує кращу інтеграцію з сучасними протоколами (наприклад, IPv6).

6. **Kerberized Internet Negotiation of Keys (KINK)**.
Забезпечує обмін ключами для IPSec із використанням протоколу автентифікації Kerberos.
*Особливості*:
– замість IKE використовує Kerberos для автентифікації та обміну ключами.
– підходить для середовищ, де вже використовується Kerberos (наприклад, корпоративні мережі).
– не потребує тривалих обмінів, характерних для IKE.
*Відмінності*:використовує централізовану модель автентифікації Kerberos замість децентралізованої схеми, властивої IKE. Власне, обмежений масштабами застосування (не підходить для відкритих мереж).

| **Протокол** | **Призначення** | **Ключова особливість** | **Шифр.** | **Автент.** |
|---|---|---|---|---|
| AH | Цілісність і автентифікація | Захист IP-заголовків | Ні | Так |
| ESP | Шифрування і цілісність | Захист корисного навантаження | Так | Так |
| ISAKMP | Управління ключами | Визначення механізмів SA | Ні | Ні |
| IKE | Управління тунелями | Двохетапний обмін | Так (з ESP) | Так |
| IKEv2 | Оптимізоване управління SA | Покращена підтримка NAT-Traversal | Так (з ESP) | Так |
| KINK | Обмін ключами з Kerberos | Централізована автентифікація | Так (з ESP) | Так |

**Таблиця 2.1** – Порівняння протоколів.

# 3 КОНЦЕПЦІЯ БЕЗПЕЧНИХ АСОЦІАЦІЙ (SECURITY ASSOCIATIONS, SA), БАЗИ ДАНИХ SPD І SAD

**Безпечна асоціація (Security Association, SA)** — це набір параметрів, які визначають, як дані шифруються, автентифікуються і передаються в межах IPSec-з'єднання. SA є ключовим елементом роботи IPSec, оскільки забезпечує конфіденційність, цілісність та автентифікацію.

**Основні аспекти SA**:
– *Односторонність*: SA працює в одному напрямку (наприклад, від вузла A до вузла B). Для двостороннього зв'язку потрібні дві SA.
– *Ідентифікація SA*: Кожна SA унікально ідентифікується трьома параметрами:

1. IP-адреса призначення.
2. Ідентифікатор протоколу безпеки (AH чи ESP).
3. SPI (Security Parameter Index)** — унікальний 32-бітний ідентифікатор.

**Параметри SA**: До параметрів входять: *Криптографічні алгоритми* (наприклад, AES для шифрування, HMAC-SHA-256 для автентифікації); *ключі* (симетричні ключі для шифрування та хешування); *термін дії* (визначає тривалість дії SA або обмеження за кількістю переданих даних); *транспортний чи тунельний режим* (визначає, чи захищаються лише дані (транспортний) або весь IP-пакет (тунельний)).

## Бази даних SPD і SAD

### Security Policy Database (SPD)

Містить політики безпеки, які визначають, як обробляти кожен IP-пакет, що проходить через IPSec.

*Призначення SPD*:
SPD вирішує, які дії виконуються для конкретного пакету:

1. DISCARD:Пакет відкидається.
2. BYPASS: Пакет передається без обробки IPSec.
3. PROTECT: Пакет обробляється відповідно до SA.

*Структура SPD*: У SPD зберігаються записи, які містять шаблони пакетів (наприклад, IP-адреси джерела та призначення, порти, протоколи); дії (визначають, чи застосовувати IPSec і як).

До способів заповнення SPD належать: ручне налаштування, коли адміністратор мережі задає політики вручну та автоматичне налаштування, коли використовуються механізми управління, наприклад, IKE.

При кожному надходженні пакету IPSec перевіряє SPD, щоб визначити, як його обробляти.

**Security Association Database (SAD)**

SAD зберігає активні SA, які були створені для обробки пакетів IPSec, зокрема:

- SPI.
- Криптографічні алгоритми та ключі.
- Параметри шифрування, автентифікації, NAT-Traversal.
- Термін дії SA.

Кожен пакет IPSec перевіряється на відповідність існуючим SA у SAD за допомогою SPI. А заповнюється він або автоматично (SA створюються під час обміну IKE/IKEv2), або у ручному налаштуванні (у разі статичної конфігурації адміністратор додає записи вручну).

**Особливості SPD і SAD у роботі IPSec**:

(а) *Взаємодія*: SPD використовується для вирішення, чи слід захищати пакет, а SAD використовується для застосування захисту відповідно до SA.

(б) *Динамічність*: політики в SPD можуть бути змінені для адаптації до нових вимог, а SAD оновлюється автоматично при зміні SA.

(в) *Захист*: SPD дозволяє виконувати тонке налаштування політик, а SAD забезпечує зберігання критично важливих параметрів SA, тому доступ до нього суворо захищений.

Концепція безпечних асоціацій (SA) є основою IPSec, забезпечуючи захищену передачу даних. SPD визначає правила, за якими пакети обробляються. У той час як SAD зберігає параметри SA для забезпечення шифрування, автентифікації та контролю. Спільна робота цих компонентів забезпечує надійну та гнучку безпеку мережевого трафіку.

# 4 ОСОБЛИВОСТІ СТРУКТУРИ ЗАГОЛОВКІВ ПРОТОКОЛІВ AH ТА ESP В ТУНЕЛЬНОМУ І ТРАНСПОРТНОМУ РЕЖИМАХ

## Протокол Authentication Header (AH)

*Структура заголовка AH*:
заголовок AH забезпечує автентифікацію, контроль цілісності та захист від повторної передачі, але не шифрує дані. AH вставляється між заголовком IP та корисним навантаженням.

| Поле | Розмір (біт) | Опис |
|---|---|---|
| Next Header | 8 | Тип наступного протоколу (TCP, UDP тощо). |
| Payload Length | 8 | Довжина заголовка AH (у 4-байтних словах). |
| Reserved | 16 | Зарезервоване для майбутнього використання (встановлюється в 0). |
| Security Parameters Index (SPI) | 32 | Унікальний ідентифікатор SA. |
| Sequence Number | 32 | Унікальний номер пакета для захисту від повторної передачі. |
| Authentication Data | Змінна | Результат хешування (HMAC) для автентифікації пакету. |

**Таблиця 4.1** – Структура заголовка AH.

*Особливості AH у режимах*:
1) транспортний режим – AH захищає лише корисне навантаження IP-пакету та його змінні поля заголовка. Структура:

$$[IPHeader][AHHeader][TCP/UDPPayload]$$

2) тунельний режим – AH захищає весь оригінальний IP-пакет, який інкапсулюється в новий. Структура:

$$[OuterIPHeader][AHHeader][InnerIPHeader + Payload]$$

*Обробка вхідних і вихідних пакетів*:
- Вихідні пакети: визначення політики в SPD. Додавання заголовка AH, обчислення HMAC, оновлення полів SPI та Sequence Number. Передача пакету на мережевий інтерфейс.
- Вхідні пакети: перевірка HMAC для автентифікації. Аналіз SPI і Sequence Number для запобігання повторним передачам. Передача корисного навантаження до вищих рівнів протоколу.

## Протокол Encapsulating Security Payload (ESP)

ESP забезпечує конфіденційність (шифрування), автентифікацію та контроль цілісності.

*Структура заголовка ESP*:

| Поле | Розмір (біт) | Опис |
|---|---|---|
| Security Parameters Index (SPI) | 32 | Ідентифікує SA. |
| Sequence Number | 32 | Унікальний номер пакета для захисту від повторної передачі. |
| Encrypted Payload | Змінна | Зашифровані дані корисного навантаження. |
| Padding | Змінна | Забезпечує вирівнювання до кратності блоку шифрування. |
| Pad Length | 8 | Довжина поля Padding. |
| Next Header | 8 | Тип протоколу (TCP, UDP тощо). |
| Integrity Check Value (ICV) | Змінна | Значення для перевірки цілісності (залежить від алгоритму хешування). |

**Таблиця 4.2** – Структура заголовка ESP.

*Особливості ESP у режимах*:

1) транспортний режим – ESP захищає лише корисне навантаження IP-пакету. Заголовок IP залишається незмінним. Структура:

$$[IPHeader][ESPHeader][EncryptedPayload + ESPTrailer][ICV]$$

2) тунельний режим – ESP захищає весь оригінальний IP-пакет, включаючи заголовок. Структура:

$$[OuterIPHeader][ESPHeader][EncryptedInnerIPHeader + Payload]$$

$$[ESPTrailer][ICV]$$

*Обробка вхідних і вихідних пакетів*:

- Вихідні пакети: визначення політики в SPD. Шифрування даних, додавання ESP Header і Trailer. Обчислення ICV і додавання до пакету. Передача пакету до мережі.

- Вхідні пакети: верифікація ICV для перевірки цілісності. Розшифрування даних, вилучення оригінального пакету. Аналіз SPI і Sequence Number для перевірки SA.

*Порівняння AH і ESP.*

| **Характеристика** | **AH** | **ESP** |
|---|---|---|
| Конфіденційність | Немає | Є |
| Цілісність | Є | Є |
| Автентифікація | Є | Є |
| Захист IP-заголовка | Частково | Повністю (у тунельному режимі) |

**Таблиця 4.3** – Порівняння AH і ESP.

*Особливості обробки пакетів*:

- Вихідні пакети: створення нового SPI і Sequence Number для кожного пакета. AH додається після IP-заголовка, ESP — перед корисним навантаженням.

- Вхідні пакети: першочергово перевіряється SPI, щоб визначити

SA. Виконується перевірка автентифікації або розшифрування залежно від протоколу.

Протоколи AH та ESP забезпечують різні аспекти безпеки в IPSec: AH надає автентифікацію та контроль цілісності, але не забезпечує конфіденційності. ESP підтримує шифрування, автентифікацію і цілісність, що робить його більш універсальним.

У транспортному режимі захищаються лише дані, тоді як у тунельному режимі — весь IP-пакет. Обробка пакетів забезпечується з використанням SAD для параметрів SA та SPD для політик.

**Особливості обробки вхідних та вихідних IPSec-пакетів для кожного з протоколів та режимів**

*Загальний процес обробки IPSec-пакетів*

IPSec забезпечує безпеку передачі даних шляхом шифрування, автентифікації, контролю цілісності та захисту від повторних передач. Процес обробки відрізняється для вхідних та вихідних пакетів, а також залежить від використаного протоколу (AH або ESP) і режиму (транспортного чи тунельного).

*Вихідні IPSec-пакети*

Основні етапи обробки:

1. *Перевірка політики в SPD (Security Policy Database)*: пакет аналізується для визначення, чи слід його захищати за допомогою IPSec:
   - якщо політика — $DISCARD$, пакет відкидається.
   - якщо $BYPASS$, передається без обробки IPSec.
   - якщо $PROTECT$, застосовуються налаштування SA.
2. *Вибір SA з SAD (Security Association Database)*: визначаються SPI, криптографічні алгоритми, ключі та режим (транспортний чи тунельний).
3. *Додавання заголовків та трейлерів*: для AH додається заголовок автентифікації, обчислюється HMAC для цілісності; для ESP пакет шифрується, додаються заголовок ESP та трейлер, а також обчислюється ICV (Integrity Check Value).
4. *Інкапсуляція у разі тунельного режиму*: оригінальний IP-пакет інкапсулюється у новий IP-заголовок
5. *Передача пакету*: пакет передається на мережевий інтерфейс для доставки.

*Обробка у транспортному режимі*

• **AH**: захищає корисне навантаження і змінні поля заголовка IP. Структура:

$$[IPHeader][AHHeader][Payload]$$

• **ESP**: шифрує лише корисне навантаження, залишаючи заголовок IP незмінним. Структура:

$$[IPHeader][ESPHeader][EncryptedPayload + ESPTrailer][ICV]$$

*Обробка у тунельному режимі*

• **AH**: захищає весь оригінальний IP-пакет. Структура:

$$[OuterIPHeader][AHHeader][InnerIPHeader + Payload]$$

• **ESP**: шифрує весь оригінальний IP-пакет, включаючи заголовок і корисне навантаження. Структура:

$$[OuterIPHeader][ESPHeader][EncryptedInnerIPHeader + Payload]$$

$$[ESPTrailer][ICV]$$

### Вхідні IPSec-пакети

*Основні етапи обробки*:

1. *Перевірка SA за SPI*: за SPI визначається, яке SA слід використовувати для обробки пакета.
2. *Перевірка цілісності*: для AH виконується перевірка HMAC для підтвердження автентичності та цілісності пакета; для ESP перевіряється ICV, якщо перевірка неуспішна, пакет відкидається.
3. *Дешифрування (для ESP)*: виконується розшифрування даних за допомогою відповідного алгоритму.
4. *Перевірка Sequence Number*: забезпечується захист від повторних атак (replay attacks). Якщо номер поза допустимим вікном, пакет відкидається.
5. *Декapsulation у разі тунельного режиму*: з оригінального пакета вилучається внутрішній IP-заголовок та корисне навантаження.
6. *Передача даних*: після успішної перевірки та обробки дані передаються вищим рівням протоколу.

*Обробка у транспортному режимі*

• **AH**: перевіряється автентичність корисного навантаження та частини заголовка IP. Структура:

$$[IPHeader][Payload]$$

• **ESP**: виконується розшифрування корисного навантаження, перевірка ICV. Структура:

$$[IPHeader][Payload]$$

*Обробка у тунельному режимі*

• **AH**: виконується перевірка автентичності всього оригінального пакета. Структура після обробки:

$$[InnerIPHeader][Payload]$$

• **ESP**: розшифровується весь оригінальний пакет, перевіряється ICV.. Структура після обробки:

$$[InnerIPHeader][Payload]$$

| **Етап обробки** | **AH** | **ESP** |
|---|---|---|
| Захист цілісності | HMAC | ICV |
| Шифрування | Немає | Так |
| Захист IP-заголовка | у транспортному режимі | у тунельному режимі |
| Перевірка Sequence Number | Так | Так |
| Розшифрування | Немає | Так |

**Таблиця 4.4** – Особливості обробки для AH та ESP.

Обробка IPSec-пакетів відрізняється залежно від:

1. *Протоколу*:

- AH забезпечує автентифікацію та контроль цілісності, але не шифрує дані.

- ESP підтримує як шифрування, так і автентифікацію.

2. *Режиму*:

- Транспортний режим захищає лише корисне навантаження пакету.

- Тунельний режим захищає весь оригінальний пакет, інкапсулюючи його в новий IP-заголовок.

Це дозволяє IPSec адаптуватися до різних сценаріїв, забезпечуючи необхідний рівень безпеки для сучасних мереж.

# 5 ДОМЕН ІНТЕРПРЕТАЦІЇ DOI

**Домен інтерпретації** (Domain of Interpretation, DOI) визначає контекст і параметри, які використовуються для узгодження безпечних асоціацій (SA) у протоколах IPSec. DOI забезпечує узгодженість між кінцевими точками, встановлюючи стандартизовані правила для інтерпретації даних під час ініціалізації та використання SA. DOI реалізується в основному у протоколах IKE (Internet Key Exchange) та IKEv2.

DOI призначається для уніфікації процесів обміну ключами та параметрами, забезпечення взаємодії між пристроями різних виробників та встановлення чітких правил для використання криптографічних алгоритмів, політик безпеки та інших параметрів IPSec.

RFC 2407 (DOI for ISAKMP) визначає такі основні компоненти DOI для IPSec:

1) *Ідентифікатори DOI*: кожен протокол або система використовує унікальний ідентифікатор DOI. Для IPSec DOI використовується значення 1.

2) *Типи протоколів*: визначає підтримувані протоколи в межах IPSec, а саме: AH (Authentication Header) – 2; ESP (Encapsulating Security Payload): – 3.

3) *Типи захищених асоціацій (SA)*: визначає типи SA: Протоколи (AH, ESP); Алгоритми (шифрування, хешування, генерація ключів).

4) *Ідентифікатори атрибутів (Attributes)*: стандартизує параметри, які використовуються в SA: типи шифрування: AES, 3DES тощо; хеш-функції: SHA-256, MD5; способи автентифікації: PSK (Pre-Shared Key), RSA, сертифікати.

5) *Механізми політик безпеки*: містить специфікації для обміну політиками безпеки, які використовуються у SPD (Security Policy Database).

6) *Повідомлення DOI*: стандартизує формати повідомлень для IKE: Payloads: SA, Proposal, Transform тощо; спеціальні типи обмінів: Main Mode, Aggressive Mode.

*Процес роботи DOI* відбувається у 4 етапи: ініціалізація SA (обмін повідомленнями між кінцевими точками для узгодження параметрів безпеки); узгодження атрибутів (обмін атрибутами, такими як SPI (Security Parameter Index), методи автентифікації, розмір ключа); формування SA (на основі узгоджених атрибутів формується SA, яка зберігається в SAD); використання SA (SA застосовується для обробки вихідних/вхідних пакетів.)

*Особливості роботи DOI у IKE/IKEv2*:

1. *IKE (Internet Key Exchange)*: визначає параметри для першої версії IKE та використовує структури, такі як SA, Proposal, Transform, для опису характеристик IPSec-з'єднання.

2. *IKEv2*: інтегрується в спрощену структуру обміну

повідомленнями та підтримує динамічну зміну параметрів SA для гнучкішої роботи.

DOI є фундаментальним компонентом архітектури IPSec, оскільки він забезпечує універсальність: дозволяє різним пристроям працювати разом, гарантує узгодженість: стандартизує інтерпретацію параметрів SA і полегшує масштабованість: підтримує різноманітні криптографічні механізми та політики.

# 6 ЗАРЕЄСТРОВАНІ АЛГОРИТМИ ДЛЯ СТЕКУ ПРОТОКОЛІВ IPSEC

IPSec підтримує широкий спектр криптографічних алгоритмів для автентифікації, шифрування та забезпечення цілісності даних. Ці алгоритми зареєстровані в різних RFC та постійно оновлюються для забезпечення актуальності й безпеки.

**Алгоритми автентифікації**
Автентифікація гарантує, що пакет походить від довіреного джерела, та перевіряє його цілісність. Основні алгоритми:

(а) *HMAC (Hash-based Message Authentication Code)*: HMAC-MD5-96: Використовує MD5 (128-бітний хеш), обмежений до 96 біт (Сьогодні не рекомендується через криптографічну слабкість MD5). HMAC-SHA-1-96: Використовує SHA-1 (160-бітний хеш), обмежений до 96 біт (Більш надійний, але вважається застарілим). HMAC-SHA-256/384/512: Використовує алгоритми SHA-2 з різними довжинами хешу (256, 384, 512 біт) (Актуальний стандарт).

(б) *AES-XCBC-MAC-96*: використовує симетричний шифр AES для автентифікації (довжина 96 біт).

(в) *GMAC (Galois Message Authentication Code)*: використовується у режимі AES-GCM (шифрування та автентифікація).

**Алгоритми шифрування**
Шифрування забезпечує конфіденційність переданих даних. Основні алгоритми:

(а) *DES (Data Encryption Standard)*: DES-CBC: Симетричний алгоритм з 56-бітним ключем. Сьогодні не використовується через низький рівень безпеки.

(б) *3DES (Triple DES)*: виконує три послідовні шифрування DES для збільшення стійкості (112-168 біт). Рідко використовується через низьку продуктивність.

(в) *AES (Advanced Encryption Standard)*: AES-CBC: Використовує 128, 192 або 256 біт ключа. AES-GCM: Забезпечує шифрування та автентифікацію в одному алгоритмі. AES-CTR: Режим лічильника для високошвидкісного шифрування. AES-GCM вважається найкращим вибором для сучасних систем.

(г) *ChaCha20-Poly1305*: високошвидкісний алгоритм, оптимізований для пристроїв із низькою продуктивністю. Альтернатива AES для мобільних пристроїв.

**Алгоритми гешування (для забезпечення цілісності)**
Геш-функції використовуються для створення перевірочних кодів (ICV).

(а) *MD5 (Message Digest 5)*: 128-бітний хеш. Вважається небезпечним для використання.

(б) *SHA-1 (Secure Hash Algorithm 1)*: 160-бітний хеш. Частково застарілий, але ще підтримується.

(в) *SHA-2*: AES-CBC: Підтримує 224, 256, 384 і 512 біт. Сучасний стандарт.

(г) *SHA-3*: Нове покоління алгоритмів гешування. Перспективний вибір.

**Алгоритми захисту від повторів (Replay Protection)**

Захист від повторних атак реалізується через механізм Sequence Number та вікна перевірки (Sliding Window).

(а) *Sequence Number*: унікальний для кожного пакета в рамках SA.

(б) *Sliding Window*: зазвичай розмір 64 або 128 записів, дозволяє фільтрувати повторювані пакети.

**Алгоритми обміну ключами**

Для ініціалізації IPSec з'єднання та обміну ключами використовуються:

(а) *Diffie-Hellman (DH)*: групи 1, 2, 5: раніше популярні, але вразливі через малий розмір ключів; групи 14, 19, 20, 21: використовують більш довгі ключі для високої стійкості; групи 31+: використовують еліптичні криві.

(б) *Elliptic Curve Diffie-Hellman (ECDH)*: Швидший і безпечніший метод обміну ключами.

(в) *Pre-Shared Key (PSK)*: Простий метод, але вразливий, якщо ключ є слабким.

(г) *RSA*: використовується для цифрового підпису та автентифікації.

**Підтримка алгоритмів в IPSec**

Згідно з RFC, IPSec визначає обов'язкові до підтримки алгоритми:

| **Тип** | **Алгоритм** | **Статус** |
|---|---|---|
| Автентифікація | HMAC-SHA-256 | Обов'язковий |
| Шифрування | AES-CBC-128 | Обов'язковий |
| Обмін ключами | Diffie-Hellman Group 14 | Обов'язковий |

**Таблиця 6.1** – Особливості обробки для AH та ESP.

# 7 ОСНОВНІ СХЕМИ ЗАСТОСУВАННЯ ПРОТОКОЛІВ IPSEC



IPSec може бути застосований у трьох основних схемах: хост-хост, шлюз-шлюз, та хост-шлюз. Кожна схема відрізняється своїм призначенням, архітектурними особливостями та сценаріями використання.

**Схема хост-хост (Host-to-Host)**

Ця схема захищає трафік між двома кінцевими хостами і використовується, коли обидві кінцеві системи підтримують IPSec. Шифрування та автентифікація відбуваються безпосередньо на кінцевих пристроях.

До переваг можна віднести максимальну безпеку, оскільки шифрування виконується на хості перед передачею даних, а також простоту реалізації для двох пристроїв.

Із недоліків це: непрактичність для масштабних мереж із великою кількістю кінцевих точок та високе навантаження на обчислювальні ресурси кінцевих пристроїв.

Сценарій застосування: захищений зв'язок між серверами, наприклад, обмін конфіденційними даними між базами даних.

**Схема шлюз-шлюз (Gateway-to-Gateway)**

Захищає трафік між двома мережами через IPSec-шлюзи, які виконують шифрування, автентифікацію та управління трафіком. А кінцеві пристрої не потребують підтримки IPSec.

Ця схема зменшує навантаження на кінцеві пристрої, легко масштабується для великих мереж та проста в управлінні політиками безпеки.

Проте, варто зазначити, що трафік у локальних мережах, до яких підключені шлюзи, не захищений і можливі вузькі місця через високий трафік на шлюзах.

Сценарії використання: захищене з'єднання між філіями організації через публічний Інтернет або VPN для з'єднання віддалених корпоративних мереж.

**Схема хост-шлюз (Host-to-Gateway)**

Захищає трафік між окремим хостом і мережею через IPSec-шлюз. Використовується, коли один із кінцевих хостів знаходиться за межами корпоративної мережі.

Дозволяє віддаленим користувачам безпечно підключатися до мережі. Підходить для мобільних пристроїв і віддалених робочих станцій.

До труднощів можна віднести: необхідність забезпечити підтримку IPSec на віддалених хостах та залежність від налаштувань шлюзу та політик безпеки.

Сценаріх використання: віддалений доступ співробітників до корпоративної мережі через VPN або захищений доступ до ресурсів у хмарі.

**Порівняльна таблиця**

| Характеристика | Хост-хост | Шлюз-шлюз | Хост-шлюз |
|---|---|---|---|
| **Призначення** | Зах траф між 2 кінцевими пристроями | Зах траф між 2 мережами | Зах траф між хостом і мережею |
| **Шифрування** | На кінцевих хостах | На шлюзах | Хост + шлюз |
| **Масштабованість** | Низька | Висока | Середня |
| **Підтримка IPSec** | На кожному хості | Тільки на шлюзах | На хості та шлюзі |
| **Продуктивність** | Залежить від ресурсів хостів | Висока, якщо шлюзи оптимізовані | Середня |
| **Сценарій** | Сервер-сервер | Мережа-мережа | Віддалений доступ |

**Таблиця 7.1** – Порівняльна таблиця.

*Примітки*:
Транспортний режим зазвичай використовується в схемі хост-хост.
Тунельний режим переважає в схемах шлюз-шлюз та хост-шлюз, оскільки шифрує весь пакет, включаючи IP-заголовок.

Кожна схема IPSec має свої переваги та недоліки, які слід враховувати залежно від архітектури мережі, вимог до безпеки та масштабованості. Для невеликих мереж або прямого з'єднання рекомендується хост-хост. Для корпоративних мереж і VPN-з'єднань краще підходять шлюз-шлюз та хост-шлюз.

# 8 IPSEC ДЛЯ ПОБУДОВИ VPN-ТУНЕЛІВ

IPSec є основною технологією для побудови віртуальних приватних мереж (VPN). Він забезпечує конфіденційність, цілісність і автентифікацію даних, переданих між двома або більше точками через незахищені мережі, такі як Інтернет. У VPN реалізується через IPSec у транспортному або тунельному режимах залежно від сценарію використання.

**Основні функції IPSec у VPN**

IPSec забезпечує конфіденційність переданих даних, щоб уникнути їх несанкціонованого прочитання завдяки шифруванню. Гарантує, що дані не змінені під час передачі, тобто цілісність даних. Підтверджує ідентичність учасників зв'язку (автентичність). Запобігає атакам повторного відтворення, аналізуючи унікальні ідентифікатори пакетів.

**Використання IPSec для VPN**

Як завжди, IPSec працює у 2 режимах:

- *Транспортний*: захищає тільки корисне навантаження IP-пакетів, не шифруючи IP-заголовки; підходить для прямого з'єднання між двома хостами (хост-хост); найчастіше використовується для внутрішньої мережі або між серверними системами.

- *Тунельний*: захищає весь IP-пакет, включаючи заголовок, інкапсулюючи його в новий IP-пакет; використовується для з'єднання між двома мережами (шлюз-шлюз) або між хостом і мережею (хост-шлюз); найбільш поширений у VPN, оскільки забезпечує максимальний рівень захисту.

**Основні етапи створення IPSec-VPN**

Їх є три штуки: *установлення захищеного з'єднання* (встановлюється між кінцевими точками через протоколи IKE або IKEv2; обираються методи шифрування та автентифікації); *створення безпечних асоціацій (SA)* (визначають параметри шифрування, цілісності та автентифікації для сесії; SA зберігаються в базі SAD); *Передача даних через IPSec-тунель* (дані інкапсулюються в IPSec-заголовки (AH або ESP) залежно від конфігурації; обробка пакетів здійснюється відповідно до політик у SPD).

**Архітектура IPSec-VPN**

| Компонент | Призначення |
|---|---|
| IPSec-шлюз | Виконує роль точки входу/виходу для захищеного трафіку. |
| Тунель IPSec | Канал для передачі зашифрованих даних між кінцевими точками. |
| Клієнт VPN | ПЗ або пристрій, що ініціює підключення до VPN, забезпечуючи аутентифікацію та шифрування. |
| SPD/SAD | Забезпечує управління політиками та параметрами для обробки пакетів. |

**Таблиця 8.1** – Архітектура IPSec-VPN.

**Особливості реалізації VPN на основі IPSec**

До особливостей реалізації на основі режиму можна сказати, що у транспортному дані шифруються, але IP-заголовки залишаються видимими і застосовується для специфічних мережевих протоколів, таких як VoIP. А у тунельному режимі весь пакет інкапсулюється, створюючи новий IP-заголовок, а використовується для Шлюз-шлюз VPN: об'єднує мережі двох офісів; Хост-шлюз VPN: дозволяє віддаленим користувачам підключатися до корпоративної мережі.

**Переваги IPSec-VPN**

Сильне шифрування та автентифікація гарантують конфіденційність і цілісність. Підтримує різні режими роботи для різних сценаріїв. Працює поверх існуючих мережевих інфраструктур.

**Недоліки IPSec-VPN**

Шифрування/дешифрування потребує значних обчислювальних потужностей. Конфігурація політик SPD і параметрів SA може бути складною. Інкапсуляція може викликати затримки у передачі даних.

**Сценарії використання**

1. **Корпоративні мережі**: об'єднання офісів компанії через шлюз-шлюз VPN.
2. **Віддалений доступ**: забезпечення захищеного підключення співробітників до корпоративних ресурсів через хост-шлюз VPN.
3. **Хмарні обчислення**: захищене підключення до хмарних платформ, таких як AWS чи Azure.

IPSec забезпечує надійний захист для VPN через гнучкість у виборі режимів роботи, підтримку сучасних криптографічних алгоритмів і відповідність вимогам до безпеки корпоративних мереж. Однак його ефективне використання потребує належного планування та налаштування.

# 9 КОНТРОЛЬНІ ЗАПИТАННЯ

1. **На якому рівні проходить функціонування протоколів IPSec згідно з мережею моделлю OSI?**
Протоколи IPSec функціонують на мережевому рівні (3-й рівень) моделі OSI, забезпечуючи захист IP-пакетів незалежно від вищих рівнів.

2. **Чи можуть протоколи IPSec використовуватися не в IP-мережах?**
Ні, протоколи IPSec розроблені виключно для IP-мереж і базуються на інкапсуляції IP-пакетів. Їх не можна використовувати безпосередньо в інших протоколах, таких як Ethernet або MPLS.

3. **Чи сумісні протоколи IPSec з протоколами IPv4 та IPv6?**
Так, IPSec є сумісним як з IPv4, так і з IPv6. У випадку IPv6 IPSec є обов'язковою частиною специфікації.

4. **Яке призначення стеку протоколів IPSec з криптографічної точки зору?**
З криптографічної точки зору, стек протоколів IPSec забезпечує: Конфіденційність (шифрування даних); Цілісність (перевірка даних на незмінність); Автентифікацію (підтвердження автентичності відправника та отримувача); Захист від повторів (перешкоджання атакам повторного відтворення).

5. **Криптографічні примітиви, які використовуються стеком протоколів IPSec**:
- *Шифрування*: AES, DES, 3DES, ChaCha20.
- *Геш-функції*: MD5, SHA-1, SHA-2 (SHA-256, SHA-512).
- *Механізми автентифікації*: HMAC, цифрові сертифікати.
- *Протоколи узгодження ключів*: Diffie-Hellman, ECDH.

6. **Основні компоненти реалізацій протоколів IPSec**:
- *Протоколи захисту*: AH (Authentication Header) і ESP (Encapsulating Security Payload).
- *Механізм узгодження ключів*: IKE/IKEv2 (Internet Key Exchange).
- *Бази даних*: SPD (Security Policy Database), SAD (Security Association Database).
- *Домен інтерпретації (DOI)*: Стандартизує параметри IPSec.

7. **Назвіть основні характеристики та відмінності протоколів AH і ESP**:
- *AH*: забезпечує автентифікацію і цілісність пакетів; не підтримує шифрування (конфіденційність); захищає IP-заголовки (у транспортному режимі).
- *ESP*: забезпечує автентифікацію, цілісність і шифрування; використовується для забезпечення конфіденційності даних; не захищає зовнішні IP-заголовки (в транспортному режимі).

8. **У чому полягають відмінності транспортного та тунельного режимів?**

- *транспортний*: захищає тільки корисне навантаження пакета (payload); використовується для хост-хост з'єднань.

- *тунельний*: інкапсулює весь IP-пакет у новий пакет із захищеним заголовком; використовується для шлюз-шлюз або хост-шлюз з'єднань.

9. **Назвіть основні зареєстровані криптографічні алгоритми протоколів IPSec**:

- *Шифрування*: AES, DES, 3DES, ChaCha20.
- *Геш-функції*: SHA-1, SHA-2 (SHA-256, SHA-384, SHA-512), MD5.
- *Механізми автентифікації*: HMAC-SHA1, HMAC-SHA256.
- *Протоколи узгодження ключів*: DH (групи 1, 2, 14, 15, 16), ECDH.

10. **У чому полягають особливості концепції безпечних асоціацій (SA)?**

SA є набором параметрів, які визначають, як саме IPSec забезпечує безпеку. Кожна SA містить алгоритми шифрування та гешування, ключі шифрування, ідентифікатор SPI (Security Parameter Index). SA є односторонньою; для двостороннього зв'язку потрібні дві SA.

11. **Як використовуються протоколи IPSec для побудови VPN-тунелів хост-хост, шлюз-шлюз та хост-шлюз?**

- *Хост-хост*: пряме з'єднання між двома комп'ютерами, яке захищає трафік на транспортному рівні.
- *Геш-функції*: захищене з'єднання між двома мережами через тунельний режим.
- *Протоколи узгодження ключів*: віддалений хост підключається до мережі через VPN, використовуючи тунельний режим для безпечного доступу до ресурсів мережі.

# ВИСНОВКИ

Дана лабораторна робота вийшла доволі об'ємною і дещо схожа на описову технічну документацію. Розглянуто усі питання, які вимагаються умовами, а саме:
описати основне призначення протоколів IPSec, їх місце в мережевій моделі OSI та взаємодію зі стеком протоколів TCP/IP та ін. Дослідити архітектуру стеку протоколів IPSec. Описати призначення, особливості та відмінності криптографічних механізмів протоколів AH, ESP, ISAKMP, IKE, IKEv2, KINK та ін. Проаналізувати концепцію безпечних асоціацій (SA), її особливості та бази даних SPD і SAD (їх призначення та способи заповнення і використання). Дослідити детально особливості структури заголовків протоколів AH і ESP в тунельному та транспортному режимах з повним описанням їх полів та можливих значень. Визначити особливості обробки вхідних та вихідних IPSec-пакетів для кожного з протоколів та режимів. Дослідити нижній рівень архітектури стеку протоколів IPSec – домен інтерпретації DOI. Визначити зареєстровані алгоритми автентифікації, шифрування, геш-функцій та ін. криптографічних алгоритмів для стеку протоколів IPSec. Визначити та описати особливості основних схем застосування протоколів IPSec: хост-хост, шлюз-шлюз та хост-шлюз. А також використання протоколів IPSec для побудови VPN-тунелів.